ELECTRONIC WATERMARK SYSTEM, METHOD FOR INSERTING/ DETECTING ELECTRONIC WATERMARK AND STORAGE MEDIUM RECORDING CONTROL PROGRAM FOR THE METHOD

Publication number: JP11327438

Publication date: 1999-11-26

Inventor: SHIBATA NAOKI; SAWADA SHUJI

Applicant: NIPPON ELECTRIC CO

Classification:

- international: ***G06F12/00; G06T1/00; G09C1/00; G09C5/00; H04L9/32; H04N1/387; H04N7/08; H04N7/081; H04N7/173;*** **G06F12/00; G06T1/00; G09C1/00; G09C5/00; H04L9/32; H04N1/387; H04N7/08; H04N7/081; H04N7/173;** (IPC1-7): G09C1/00; G06F12/00; G06T1/00; G09C5/00; H04N1/387; H04N7/08; H04N7/081; H04N7/173

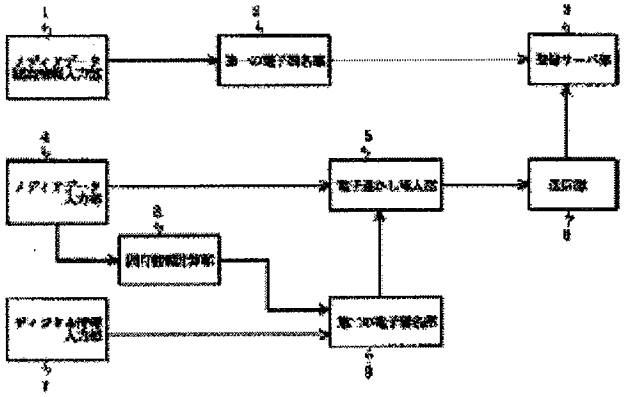
- European:

Application number: JP19980129378 19980513

Priority number(s): JP19980129378 19980513

Abstract of **JP11327438**

PROBLEM TO BE SOLVED: To provide an electronic watermark system capable of preventing original medium data and an embedded electronic water mark from being easily separated from each other without allowing much original medium data to flow out and capable of specifying an alterator even when the insertion/detection or the like of an electronic watermark is distributed to plural servers or clients. SOLUTION: A 1st electronic signature part 2 electronically signs inherent information inputted from a medium data inherent information input part 1. An inherent information calculation part 8 calculates the inherent information of medium data inputted from a medium data input part 4. A 2nd electronic signature part 9 electronically signs synthetic information synthesized from digital information inputted from a digital information input part 7 and the inherent information from the calculation part 8. An electronic watermark inserting part 5 embeds the electrically signed synthetic information in the medium data. When inherent information in data transmitted from a transmission part 6 coincides with the inherent information outputted from the 1st electronic signature part 2, a registration server part 3 registers the medium data.



Family list
2 family member for: **JP11327438**
Derived from 1 application

Back to JP1132

1 **ELECTRONIC WATERMARK SYSTEM, METHOD FOR INSERTING/ DETECTING ELECTRONIC WATERMARK AND STORAGE MEDIUM RECORDING CONTROL PROGRAM FOR THE METHOD**

Inventor: SHIBATA NAOKI; SAWADA SHUJI **Applicant:** NIPPON ELECTRIC CO

EC: **IPC:** ***G06F12/00; G06T1/00; G09C1/00*** (+23)

Publication info: **JP3104676B2 B2** - 2000-10-30
JP11327438 A - 1999-11-26

Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－327438

(43)公開日　平成11年(1999)11月26日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｃ０９Ｃ　1/00	６４０Ｂ
Ｇ０６Ｆ　12/00	５３７	Ｃ０６Ｆ　12/00	５３７Ｈ
Ｇ０６Ｔ　1/00		Ｇ０９Ｃ　5/00	
Ｇ０９Ｃ　5/00		Ｈ０４Ｎ　1/387	
Ｈ０４Ｎ　1/387		7/173	

審査請求　有　請求項の数21　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平10－129378

(22)出願日　平成10年(1998)５月13日

特許法第30条第１項適用申請有り　1998年３月13日　画像電子学会開催の「第162回研究会」において文書をもって発表

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　柴多　直樹
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　澤田　修司
東京都港区芝五丁目７番１号　日本電気株式会社内

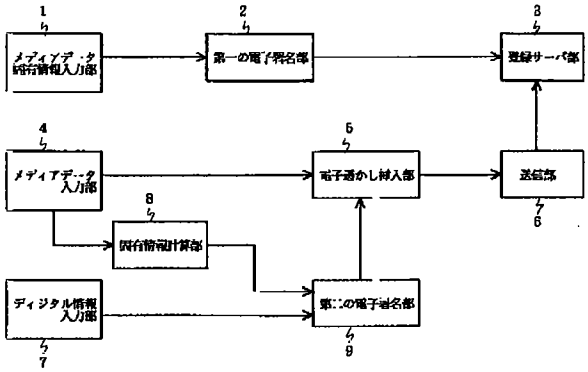
(74)代理人　弁理士　▲柳▼川　信

(54)【発明の名称】　電子透かしシステム及びその電子透かし挿入・検出方法並びにその制御プログラムを記録した記録媒体

(57)【要約】

【課題】　元のメディアデータをあまり流出させることなく、元のメディアデータと埋め込まれた電子透かしとを分離しにくくし、電子透かしの挿入・検出等を複数のサーバやクライアントに分散した場合でも改竄者を特定可能な電子透かしシステムを提供する。

【解決手段】　第一の電子署名部２はメディアデータ固有情報入力部１からの固有情報に電子署名を施す。固有情報計算部８はメディアデータ入力部４からのメディアデータの固有情報を計算する。第二の電子署名部９はディジタル情報入力部７からのディジタル情報と固有情報計算部８からの固有情報との合成情報に電子署名を施す。電子透かし挿入部５はメディアデータに電子署名が施された合成情報を埋込む。登録サーバ部３は送信部６からのデータ内の固有情報と第一の電子署名部２からの固有情報とが一致した時にメディアデータを登録する。



【特許請求の範囲】

【請求項１】　メディアデータに電子透かしを挿入する電子透かし挿入システムであって、外部から入力されかつ前記メディアデータを特定する固有情報に第一の電子署名を施す第一の電子署名手段と、外部から入力された前記メディアデータから前記メディアデータを特定する固有情報を計算する固有情報計算手段と、前記固有情報計算手段の計算結果と前記メディアデータに添付すべき添付情報との合成情報に第二の電子署名を施す第二の電子署名手段と、前記第二の電子署名手段で前記第二の電子署名が施こされた前記合成情報を前記電子透かしとして前記メディアデータに埋込む電子透かし挿入手段と、前記第一の電子署名手段で前記第一の電子署名が施こされた固有情報と前記第二の電子署名手段で前記第二の電子署名が施こされた固有情報とを比較しかつその比較結果に応じて前記メディアデータをデータベースに登録する登録サーバとを有することを特徴とする電子透かし挿入システム。

【請求項２】　前記第一の電子署名は、前記登録サーバを利用する第一の利用者を特定する情報であり、
前記第２の電子署名は、前記登録サーバに前記メディアデータを登録する第二の利用者を特定する情報であることを特徴とする請求項１記載の電子透かし挿入システム。

【請求項３】　前記登録サーバは、入力されたメディアデータから前記電子透かしを抽出する抽出機能と、前記抽出機能で抽出された前記電子透かしの固有情報と前記第一の電子署名手段で前記第一の電子署名が施こされた固有情報とを比較する比較機能とを含み、前記比較機能で一致が検出された時に当該メディアデータを前記データベースに登録するよう構成したことを特徴とする請求項１または請求項２記載の電子透かし挿入システム。

【請求項４】　入力されるメディアデータから電子透かしを検出する電子透かし検出システムであって、入力されたメディアデータから前記電子透かしを抽出する電子透かし抽出手段と、前記メディアデータから前記電子透かし抽出手段で抽出された電子透かしを除去して前記メディアデータのみを作成する作成手段と、前記作成手段で前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算する固有情報計算手段と、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースと、前記固有情報計算手段で計算された固有情報を基に前記データベースから当該固有情報に対応する添付情報を検索する検索手段と、前記固有情報計算手段で計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かし抽出手段で抽出された電子透かしに対するデコード処理を行う署名デコード手段と、前記署名デコード手段のデコード結果と前記検索手段の検索結果とを比較する比較手段と、前記比較手段の比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力する出力選択手段とを有することを特徴とした電子透かし検出システム。

【請求項５】　前記検出手段は、前記固有情報計算手段で計算された固有情報と前記データベースから検索された前記添付情報との合成情報のハッシュ値を計算する計算機能を含み、
前記署名デコード手段は、前記電子透かし抽出手段で抽出された電子透かしをデコードすることで前記合成情報のハッシュ値を出力するよう構成したことを特徴とする請求項４記載の電子透かし検出システム。

【請求項６】　複数の検出システムからなり、前記複数の検出システム各々において入力されるメディアデータから電子透かしを検出する電子透かし検出システムであって、
入力されたメディアデータから前記電子透かしを抽出する電子透かし抽出手段と、前記メディアデータから前記電子透かし抽出手段で抽出された電子透かしを除去して前記メディアデータのみを作成する作成手段と、前記作成手段で前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算する固有情報計算手段と、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースと、前記固有情報計算手段で計算された固有情報を基に前記データベースから当該固有情報に対応する添付情報を検索する検索手段と、前記固有情報計算手段で計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かし抽出手段で抽出された電子透かしに対するデコード処理を行う署名デコード手段と、前記署名デコード手段のデコード結果と前記検索手段の検索結果とを比較する比較手段と、前記比較手段の比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力する出力選択手段とを前記複数の検出システム各々に有し、
前記複数の検出システム各々の前記出力選択手段からの出力に対して多数決をとる多数決手段を有することを特徴とする電子透かし検出システム。

【請求項７】　前記検出手段は、前記固有情報計算手段で計算された固有情報と前記データベースから検索された前記添付情報との合成情報のハッシュ値を計算する計算機能を含み、
前記署名デコード手段は、前記電子透かし抽出手段で抽出された電子透かしをデコードすることで前記合成情報のハッシュ値を出力するよう構成したことを特徴とする請求項６記載の電子透かし検出システム。

【請求項８】　メディアデータに電子透かしを挿入する

電子透かし挿入方法であって、外部から入力されかつ前記メディアデータを特定する固有情報に第一の電子署名を施すステップと、外部から入力された前記メディアデータから前記メディアデータを特定する固有情報を計算するステップと、その計算された固有情報と前記メディアデータに添付すべき添付情報との合成情報に第二の電子署名を施すステップと、前記第二の電子署名が施こされた前記合成情報を前記電子透かしとして前記メディアデータに埋込むステップと、前記第一の電子署名が施こされた固有情報と前記第二の電子署名が施こされた固有情報とを比較しかつその比較結果に応じて前記メディアデータをデータベースに登録するステップとを有することを特徴とする電子透かし挿入方法。

【請求項９】　前記第一の電子署名を施すステップは、前記登録サーバを利用する第一の利用者を特定する情報を前記第一の電子署名として前記固有情報に施し、

前記第２の電子署名を施すステップは、前記登録サーバに前記メディアデータを登録する第二の利用者を特定する情報を前記第二の電子署名として前記合成情報に施すようにしたことを特徴とする請求項８記載の電子透かし挿入方法。

【請求項１０】　前記メディアデータを前記データベースに登録するステップは、入力されたメディアデータから前記電子透かしを抽出し、その抽出された前記電子透かしの固有情報と前記第一の電子署名が施こされた固有情報とを比較し、その比較で一致が検出された時に当該メディアデータを前記データベースに登録するようにしたことを特徴とする請求項８または請求項９記載の電子透かし挿入方法。

【請求項１１】　入力されるメディアデータから電子透かしを検出する電子透かし検出方法であって、入力されたメディアデータから前記電子透かしを抽出するステップと、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成するステップと、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算するステップと、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行うステップと、計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かしに対するデコード処理を行うステップと、前記デコード処理の結果と前記検索処理の結果とを比較するステップと、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力するステップとを有することを特徴とした電子透かし検出方法。

【請求項１２】　前記検索処理を行うステップは、計算された固有情報と前記データベースから検索された前記添付情報との合成情報のハッシュ値を計算し、

前記デコード処理を行うステップは、抽出された電子透かしをデコードすることで前記合成情報のハッシュ値を出力するようにしたことを特徴とする請求項１１記載の電子透かし検出方法。

【請求項１３】　複数の検出システムからなり、前記複数の検出システム各々において入力されるメディアデータから電子透かしを検出する電子透かし検出システムの電子透かし検出方法であって、

入力されたメディアデータから前記電子透かしを抽出するステップと、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成するステップと、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算するステップと、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行うステップと、計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かしに対するデコード処理を行うステップと、前記デコード処理の結果と前記検索処理の結果とを比較するステップと、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力するステップとを前記複数の検出システム各々に有し、

前記複数の検出システム各々の前記出力選択手段からの出力に対して多数決をとるステップを有することを特徴とする電子透かし検出方法。

【請求項１４】　前記検索処理を行うステップは、計算された固有情報と前記データベースから検索された前記添付情報との合成情報のハッシュ値を計算し、

前記デコード処理を行うステップは、抽出された電子透かしをデコードすることで前記合成情報のハッシュ値を出力するようにしたことを特徴とする請求項１４記載の電子透かし検出方法。

【請求項１５】　コンピュータにメディアデータへの電子透かしの挿入を行わせるための電子透かし挿入制御プログラムを記録した記録媒体であって、前記電子透かし挿入制御プログラムは前記コンピュータに、外部から入力されかつ前記メディアデータを特定する固有情報に第一の電子署名を施させ、外部から入力された前記メディアデータから前記メディアデータを特定する固有情報を計算させ、その計算された固有情報と前記メディアデータに添付すべき添付情報との合成情報に第二の電子署名を施させ、前記第二の電子署名が施こされた前記合成情報を前記電子透かしとして前記メディアデータに埋込ませ、前記第一の電子署名が施こされた固有情報と前記第二の電子署名が施こされた固有情報とを比較させかつその比較結果に応じて前記メディアデータをデータベース

に登録させることを特徴とする電子透かし挿入制御プログラムを記録した記録媒体。

【請求項16】　前記電子透かし挿入制御プログラムは前記コンピュータに、前記第一の電子署名を施させる際に、前記登録サーバを利用する第一の利用者を特定する情報を前記第一の電子署名として前記固有情報に施させ、

前記第2の電子署名を施させる際に、前記登録サーバに前記メディアデータを登録する第二の利用者を特定する情報を前記第二の電子署名として前記合成情報に施させることを特徴とする請求項15記載の電子透かし挿入制御プログラムを記録した記録媒体。

【請求項17】　前記電子透かし挿入制御プログラムは前記コンピュータに、前記メディアデータを前記データベースに登録させる際に、入力されたメディアデータから前記電子透かしを抽出させ、その抽出された前記電子透かしの固有情報と前記第一の電子署名が施こされた固有情報とを比較させ、その比較で一致が検出された時に当該メディアデータを前記データベースに登録させるようにしたことを特徴とする請求項15または請求項16記載の電子透かし挿入制御プログラムを記録した記録媒体。

【請求項18】　コンピュータに、入力されるメディアデータから電子透かしを検出させるための電子透かし検出制御プログラムを記録した記録媒体であって、前記電子透かし検出制御プログラムは前記コンピュータに、入力されたメディアデータから前記電子透かしを抽出させ、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成させ、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算させ、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行わせ、計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かしに対するデコード処理を行わせ、前記デコード処理の結果と前記検索処理の結果とを比較させ、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力させることを特徴とした電子透かし検出制御プログラムを記録した記録媒体。

【請求項19】　前記電子透かし検出制御プログラムは前記コンピュータに、前記検索処理を行わせる際に、計算された固有情報と前記データベースから検索された前記添付情報との合成情報のハッシュ値を計算させ、

前記デコード処理を行わせる際に、抽出された電子透かしをデコードすることで前記合成情報のハッシュ値を出力させることを特徴とする請求項18記載の電子透かし検出制御プログラムを記録した記録媒体。

【請求項20】　複数の検出システム各々のコンピュータに、入力されるメディアデータから電子透かしを検出させるための電子透かし検出制御プログラムを記録した記録媒体であって、

前記電子透かし検出制御プログラムは前記複数の検出システム各々のコンピュータに、入力されたメディアデータから前記電子透かしを抽出させ、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成させ、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算させ、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行わせ、計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かしに対するデコード処理を行わせ、前記デコード処理の結果と前記検索処理の結果とを比較させ、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力させ、

前記複数の検出システム各々のコンピュータからの出力に対して多数決をとるようにしたことを特徴とする電子透かし検出制御プログラムを記録した記録媒体。

【請求項21】　前記電子透かし検出制御プログラムは前記複数の検出システム各々のコンピュータに、前記検索処理を行わせる際に、計算された固有情報と前記データベースから検索された前記添付情報との合成情報のハッシュ値を計算させ、前記デコード処理を行わせる際に、抽出された電子透かしをデコードすることで前記合成情報のハッシュ値を出力させることを特徴とする請求項20記載の電子透かし検出制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は電子透かしシステム及びその電子透かし挿入・検出方法並びにその制御プログラムを記録した記録媒体に関し、特に電子透かし挿入・検出装置における電子透かしの改竄検出方法に関する。

【0002】

【従来の技術】従来、電子透かし技術においては、主として元のメディアの情報（主信号）に電子透かしの情報（副信号）を挿入すること、あるいは信号処理的にメディアデータに改竄が加えられた時の検出性能に主眼がおかれている。

【0003】例えば、「ウェーブレットを利用したクリップ画像からの署名検出法」（大西淳児・松井甲子雄・小沢慎治著、1997年電子情報通信学会基礎・境界ソサイエティ大会SA－7－1）（以下、文献1とする）

には、スペクトラム拡散の手法で静止画というメディアデータに電子透かしを入れる場合の画像処理的改竄への防御策が述べられている。

【０００４】また、「ブラインド電子透かしの提案」（岩村恵市・桜井幸一・今井秀樹著、信学技報ＩＳＥＣ９７－３５、１９９７－０９）（以下、文献２とする）や「通信量を考慮したサーバの不正行為も防止する電子透かしシステム」（三浦信治・大西重行・渡辺創・嵩忠雄著、信学技報ＩＳＥＣ９７－３６、１９９７－０９）（以下、文献３とする）では、電子署名を用いることによって改竄等の不正を検出することを狙っている。

【０００５】さらに、「公開鍵暗号に基づくセキュア電子透かしシステム」（吉浦裕・宝木和夫・佐々木良一著、１９９７年電子情報通信学会基礎・境界ソサイエティ大会ＳＡ－７－７）（以下、文献４とする）でも電子透かし及び工学的改竄防止措置によって改竄を防止することを狙っている。

【０００６】

【発明が解決しようとする課題】上述した従来の電子透かし技術では、文献１に代表される信号処理レベルの改竄対策の場合、透かしとして埋込む副情報の内容について触れられていない。例えば、文献１の方法では透かしの検出に際して元の画像を用いているが、検出時に元の画像が本当に元の画像であるかどうかのチェックについては言及していないため、改竄を行おうとすれば、原画像と偽って別な透かしが入っている画像を準備することもできる。

【０００７】文献２，３の方法では特定の電子透かし挿入・検出技法によらずに改竄を防止するのに、電子署名を電子透かしデータとして埋込む等の方法を取っている。しかしながら、文献２，３の方法で想定している電子透かし挿入はメディアデータをスクランブル処理した場合にも電子透かしが変換に対して不変であるという仮定によっている。現在まで発表されている電子透かし挿入・検出技術ではスクランブル前後で変わらない電子透かしは実現されておらず、実現の可能性に疑問が残る。また、メディアの原データ、例えば画像の場合には原画像を作者以外の者が所持するので、それを回避するためにスクランブル等を必要としている。

【０００８】文献４の方法ではＩＣカード等の工学的な防御手段を講じて改竄を不可能とする方法が提案されている。電子透かしを入れさせたい側と電子透かしに不正が無いことを監視したい側が、購入者の側でＩＣカード内で電子透かしを挿入している。しかしながら、結局、これは電子透かしを入れさせたい側で準備したＩＣカードの中での電子透かし挿入が電子透かしを入れさせたい側で挿入しているのと変わらず、自体はあまり改善されていない。

【０００９】そこで、本発明の目的は上記の問題点を解消し、元のメディアデータをあまり流出させることなく、元のメディアデータと埋め込まれた電子透かしとを分離しにくくすることができ、電子透かしの挿入・検出等を複数のサーバやクライアントに分散した場合でも改竄者を特定することができる電子透かしシステム及びその電子透かし挿入・検出方法並びにその制御プログラムを記録した記録媒体を提供することにある。

【００１０】

【課題を解決するための手段】本発明による電子透かし挿入システムは、メディアデータに電子透かしを挿入する電子透かし挿入システムであって、外部から入力されかつ前記メディアデータを特定する固有情報に第一の電子署名を施す第一の電子署名手段と、外部から入力された前記メディアデータから前記メディアデータを特定する固有情報を計算する固有情報計算手段と、前記固有情報計算手段の計算結果と前記メディアデータに添付すべき添付情報との合成情報に第二の電子署名を施す第二の電子署名手段と、前記第二の電子署名手段で前記第二の電子署名が施こされた前記合成情報を前記電子透かしとして前記メディアデータに埋込む電子透かし挿入手段と、前記第一の電子署名手段で前記第一の電子署名が施こされた固有情報と前記第二の電子署名手段で前記第二の電子署名が施こされた固有情報とを比較しかつその比較結果に応じて前記メディアデータをデータベースに登録する登録サーバとを備えている。

【００１１】本発明による電子透かし検出システムは、入力されるメディアデータから電子透かしを検出する電子透かし検出システムであって、入力されたメディアデータから前記電子透かしを抽出する電子透かし抽出手段と、前記メディアデータから前記電子透かし抽出手段で抽出された電子透かしを除去して前記メディアデータのみを作成する作成手段と、前記作成手段で前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算する固有情報計算手段と、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースと、前記固有情報計算手段で計算された固有情報を基に前記データベースから当該固有情報に対応する添付情報を検索する検索手段と、前記固有情報計算手段で計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かし抽出手段で抽出された電子透かしに対するデコード処理を行う署名デコード手段と、前記署名デコード手段のデコード結果と前記検索手段の検索結果とを比較する比較手段と、前記比較手段の比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力する出力選択手段とを備えている。

【００１２】本発明による他の電子透かし検出システムは、複数の検出システムからなり、前記複数の検出システム各々において入力されるメディアデータから電子透

かしを検出する電子透かし検出システムであって、入力されたメディアデータから前記電子透かしを抽出する電子透かし抽出手段と、前記メディアデータから前記電子透かし抽出手段で抽出された電子透かしを除去して前記メディアデータのみを作成する作成手段と、前記作成手段で前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算する固有情報計算手段と、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースと、前記固有情報計算手段で計算された固有情報を基に前記データベースから当該固有情報に対応する添付情報を検索する検索手段と、前記固有情報計算手段で計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かし抽出手段で抽出された電子透かしに対するデコード処理を行う署名デコード手段と、前記署名デコード手段のデコード結果と前記検索手段の検索結果とを比較する比較手段と、前記比較手段の比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力する出力選択手段とを前記複数の検出システム各々に備え、前記複数の検出システム各々の前記出力選択手段からの出力に対して多数決をとる多数決手段を備えている。

【００１３】本発明による電子透かし挿入方法は、メディアデータに電子透かしを挿入する電子透かし挿入方法であって、外部から入力されかつ前記メディアデータを特定する固有情報に第一の電子署名を施すステップと、外部から入力された前記メディアデータから前記メディアデータを特定する固有情報を計算するステップと、その計算された固有情報と前記メディアデータに添付すべき添付情報との合成情報に第二の電子署名を施すステップと、前記第二の電子署名が施こされた前記合成情報を前記電子透かしとして前記メディアデータに埋込むステップと、前記第一の電子署名が施こされた固有情報と前記第二の電子署名が施こされた固有情報とを比較しかつその比較結果に応じて前記メディアデータをデータベースに登録するステップとを備えている。

【００１４】本発明による電子透かし検出方法は、入力されるメディアデータから電子透かしを検出する電子透かし検出方法であって、入力されたメディアデータから前記電子透かしを抽出するステップと、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成するステップと、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算するステップと、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行うステップと、計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かしに対するデコード処理を行うステップと、前記デコード処理の結果と前記検索処理の結果とを比較するステップと、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力するステップとを備えている。

【００１５】本発明による他の電子透かし検出方法は、複数の検出システムからなり、前記複数の検出システム各々において入力されるメディアデータから電子透かしを検出する電子透かし検出システムの電子透かし検出方法であって、入力されたメディアデータから前記電子透かしを抽出するステップと、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成するステップと、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算するステップと、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行うステップと、計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かしに対するデコード処理を行うステップと、前記デコード処理の結果と前記検索処理の結果とを比較するステップと、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力するステップとを前記複数の検出システム各々に備え、前記複数の検出システム各々の前記出力選択手段からの出力に対して多数決をとるステップを備えている。

【００１６】本発明による電子透かし挿入制御プログラムを記録した記録媒体は、コンピュータにメディアデータへの電子透かしの挿入を行わせるための電子透かし挿入制御プログラムを記録した記録媒体であって、前記電子透かし挿入制御プログラムは前記コンピュータに、外部から入力されかつ前記メディアデータを特定する固有情報に第一の電子署名を施させ、外部から入力された前記メディアデータから前記メディアデータを特定する固有情報を計算させ、その計算された固有情報と前記メディアデータに添付すべき添付情報との合成情報に第二の電子署名を施させ、前記第二の電子署名が施こされた前記合成情報を前記電子透かしとして前記メディアデータに埋込ませ、前記第一の電子署名が施こされた固有情報と前記第二の電子署名が施こされた固有情報とを比較させかつその比較結果に応じて前記メディアデータをデータベースに登録させている。

【００１７】本発明による電子透かし検出制御プログラムを記録した記録媒体は、コンピュータに、入力されるメディアデータから電子透かしを検出させるための電子透かし検出制御プログラムを記録した記録媒体であっ

て、前記電子透かし検出制御プログラムは前記コンピュータに、入力されたメディアデータから前記電子透かしを抽出させ、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成させ、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算させ、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行わせ、計算された固有情報を基に前記データベースから検索した電子署名に基づいて前記電子透かしに対するデコード処理を行わせ、前記デコード処理の結果と前記検索処理の結果とを比較させ、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力させている。

【００１８】本発明による他の電子透かし検出制御プログラムを記録した記録媒体は、複数の検出システム各々のコンピュータに、入力されるメディアデータから電子透かしを検出させるための電子透かし検出制御プログラムを記録した記録媒体であって、前記電子透かし検出制御プログラムは前記複数の検出システム各々のコンピュータに、入力されたメディアデータから前記電子透かしを抽出させ、その抽出された電子透かしを前記メディアデータから除去して前記メディアデータのみを作成させ、前記電子透かしが除去されたメディアデータを基に当該メディアデータの固有情報を計算させ、前記メディアデータの固有情報と前記メディアデータに添付すべき添付情報と前記固有情報及び前記添付情報の合成情報に施される電子署名とを少なくとも蓄積するデータベースから前記固有情報を基に当該固有情報に対応する添付情報の検索処理を行わせ、計算された固有情報を基に前記データベースから検索した電子署名を基に前記電子透かしに対するデコード処理を行わせ、前記デコード処理の結果と前記検索処理の結果とを比較させ、この比較結果に応じて少なくとも前記データベースから検索されたデータの出力の可否を決定して出力させ、前記複数の検出システム各々のコンピュータからの出力に対して多数決をとるようにしている。

【００１９】すなわち、本発明の電子透かしシステムは、メディアデータに電子透かしを挿入するシステムであり、メディアデータの固有情報の入力時にその固有情報にメディアデータの供給者の電子署名を施して保持しておく。

【００２０】また、上記のメディアデータの登録時にそのメディアデータから計算した固有情報と当該メディアデータの登録者が入力したディジタル情報とにその登録者の電子署名を施して当該メディアデータに電子透かしとして埋込む。

【００２１】当該メディアデータが登録される登録サーバでは当該メディアデータの供給者側からの固有情報と、当該メディアデータの登録者側から送られてきたメディアデータに電子透かしとして埋込まれた固有情報とを比較し、一致した時のみ当該メディアデータをデータベースに蓄積する。

【００２２】一方、メディアデータから電子透かしを検出するシステムでは入力されるメディアデータから電子透かしを抽出するとともに、そのメディアデータから電子透かしを除去してメディアデータを作成する。

【００２３】当該電子透かしが除去されたメディアデータからメディアデータの固有情報を求め、その固有情報をキーとしてデータベースから検索したデータを電子署名のキーとし、抽出された電子透かしに対して当該電子署名のキーでデコード処理を行う。

【００２４】上記の処理で求められた固有情報と当該固有情報を検索キーとしてデータベースから検索された情報よりハッシュ値を計算し、このハッシュ値を上記のデコード処理で得られたデコード結果と比較し、その比較結果を基にデータベースから検索された結果の一部または全てのデータの出力の可否を決定して出力する。

【００２５】また、メディアデータから電子透かしを検出するシステムでは、メディアデータからの電子透かしの検出時に上記の検出方法を用いたシステムを二つ以上利用し、その一つ以上のシステムの結果を統合あるいは一部を選択している。

【００２６】これによって、電子透かしとメディアデータ自身の関係を電子透かしの一部として取入れ、さらに電子署名を施すことによって、電子透かしとメディアデータとを分離したり、内容を改竄したりすることを困難とすることが可能となる。

【００２７】また、元のメディアデータの配布範囲を必要最小限としているために、原メディアデータの流出をより強く防止することが可能となる。さらに、メディアデータからの電子透かしの検出結果を多数決で判定することで、特定のサーバの不正が防止しやすくなる。

【００２８】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例による電子透かしシステムの構成を示すブロック図である。図において、本発明の一実施例による電子透かしシステムはメディアデータ固有情報入力部１と、第一の電子署名部２と、登録サーバ部３と、メディアデータ入力部４と、電子透かし挿入部５と、送信部６と、ディジタル情報入力部７と、固有情報計算部８と、第二の電子署名部９とから構成されている。

【００２９】メディアデータ固有情報入力部１からは電子透かしを挿入するメディアデータの固有情報が入力される。ここで、メディアデータとは静止画や動画、及び音声といったデータである。

【００３０】また、メディアの固有情報とはそれらのデ

ータを十分に特定することができる情報である。具体的には、例えばメディアデータが静止画の場合、その固有情報としては画像をブロック単位に細分化し、各ブロックでＤＣＴ（Ｄｉｓｃｒｅｔｅ　Ｃｏｓｉｎｅ　Ｔｒａｎｓｆｏｒｍ）係数を求め、その低周波成分を固有情報とする等の方法がある。この方法については、「画像情報のデジタル署名の一実現法」（亀屋雅樹・田中初一著、１９９３年暗号と情報セキュリティシンポジウム・シンポジウム資料、ＳＣＩＳ９３－１３Ａ、１９９３年）（以下、文献５とする）等に開示された方法がある。

【００３１】他には研究レベルであるが、画像の中のエッジやコーナ等の注視点をフィルタによって検出してその付近の何らかの特徴量を求めて固有情報とすることもできる。これらの方法については、固有情報がメディアデータを特定することができればよく、特に一つの方法に限定する必要はなく、固有情報の計算の仕方自体が本発明の目的ではないので、それらの方法の詳細な説明は省略する。

【００３２】第一の電子署名部２はメディアデータ固有情報入力部１から入力された固有情報に、そのメディアデータの供給者の電子署名を施し、その情報を登録サーバ部３に出力する。電子署名の方法等については、例えば「現代暗号」（岡本龍明、山本博資著、産業図書、１９９７年）等に詳細に記述されている。また、電子署名はディジタル署名や電子印鑑等とも呼ばれており、ＲＳＡ署名等をはじめとして様々な方式が提案されている。

【００３３】本発明においては秘密鍵と公開鍵とを用いる方式であれば、どの様な方式を用いても構わない。また、本発明の一実施例による電子透かしシステムで用いる電子署名の方式はハッシュを使うことを想定している。つまり、第一の電子署名部２では固有情報のハッシュ値を求め、そのハッシュ値にメディアデータの供給者の電子署名を施すこととなる。

【００３４】メディアデータ入力部４は電子透かしを挿入するメディアデータの入力手段である。これは、例えばメディアデータが静止画の場合、ＪＰＥＧ（ＪｏｉｎｔＰｈｏｔｏｇｒａｐｈｉｃ　ｃｏｄｉｎｇ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）やＴＩＦＦ（Ｔａｇ　Ｉｍａｇｅ　Ｆｉｌｅ　Ｆｏｒｍａｔ）といったフォーマットのデータを入力する手段にあたる。より具体的には、例えばコンピュータ上のディスク装置やネットワーク等のデータ入力手段、あるいはスキャナ装置等を用いた画像取込み手段に相当する。

【００３５】固有情報計算部８はメディアデータ入力部４から入力されたメディアデータの固有情報を計算する。この固有情報とは上述したように、メディアデータを特定する情報である。メディアデータ固有情報入力部１から入力される固有情報の計算には固有情報計算部８と同様の計算手段（図示せず）が用いられる。

【００３６】ディジタル情報入力部７からはテキストデータやバイナリデータ、あるいはそれらの組合せが入力する。第二の電子署名部９は第一の電子署名部２と同様の方法で、ディジタル情報入力部７からのディジタル情報と固有情報計算部８で計算された固有情報とを合成した情報に電子署名を施し、その情報を電子透かし挿入部５に出力する。つまり、第二の電子署名部９ではディジタル情報と固有情報との合成情報のハッシュ値を求め、そのハッシュ値にメディアデータの登録者の電子署名を施すこととなる。

【００３７】ディジタル情報入力部７からのディジタル情報と固有情報計算部８で計算された固有情報とを合成する方法としては様々な方法が考えられる。もっとも単純な方法としては、固有情報計算部８からの出力データの最後部にディジタル情報入力部７からのディジタル情報をアペンドしたものを一つのデータとして電子署名を施す。この場合の順序は逆でも構わない。

【００３８】また、どちらかの情報があきらかに大きい場合には、サイズが大きなデータに小さい方のデータをインタリーブしてもよい。他にも二つのデータを合成する方法としては様々な方法が考えられるが、それらの情報を合成することが本発明の目的ではないので、合成方法についての詳細な説明は省略する。

【００３９】電子透かし挿入部５はメディアデータ入力部４から入力されたメディアデータを電子透かしを埋めるための主情報とし、第二の電子署名部９で得られた電子署名付きの固有情報及びディジタル情報入力部７から入力されたディジタル情報をメディアデータに埋込む電子透かし、すなわち副情報として、電子透かしを埋込んだメディアデータを作成する。

【００４０】電子透かしを挿入する方法としては、例えば特開平９－１９１３９４号公報や国際公開特許ＷＯ９５／１４２８９　“Ｉｄｅｎｔｉｆａｃｔａｉｏｎ／ａｕｔｈｅｎｔｉｆｉｃａｔｉｏｎ　ｃｏｄｉｎｇ　ｍｅｔｈｏｄ　ａｎｄ　ａｐｐａｒａｔｕｓ”、「デジタル画像の著作権保護の為の周波数領域における電子透かし方式」（電子通信学会暗号と情報セキュリティシンポジウム（ＳＣＩＳ）９７，ＳＣＩＳ９７－２６Ａ）等に開示されている方法を用いることができる。

【００４１】送信部６は電子透かし挿入部５で電子透かしが挿入されたデータ、ディジタル情報、固有情報のデータを一まとめにし、さらにそのデータ全体に対して電子署名を施して登録サーバ部３に送信する。

【００４２】これは、例えばイーサネット接続されたＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）上で、適当なプロトコルを利用あるいは作成し、サーバにデータを送信する。比較的上位のレイヤのプロトコルとしては、例えばＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）（メール送信）等を用いてデータを送信することも可能である。通信路上での

守秘のためにこれらの送信データを暗号化すること等が考えられるが、それは本発明の目的とするところではないので、その詳細な説明は省略する。

【００４３】登録サーバ部３は第一の電子署名部２で電子署名が施された第一の固有情報データを受取り、また送信部６からのディジタル情報及び第二の固有情報データが電子透かしとして付加された情報を受取る。

【００４４】登録サーバ部３はこれらの情報を受取ると、第一の固有情報データと第二の固有情報データとを比較し、それらが一致した時に送信部６から送られてきた電子署名、電子透かしが入ったメディアデータ、ディジタル情報、固有情報を夫々図示せぬデータベースに記録する。

【００４５】図２は本発明の一実施例による電子透かしシステムのシステム構成を示すブロック図である。図において、第一の単体コンピュータ１１上には上記のメディアデータ固有情報入力部１及び第一の電子署名部２が構成され、第二の単体コンピュータ１２上には登録サーバ部３が構成され、第三の単体コンピュータ１２上にはメディアデータ入力部４と電子透かし挿入部５と送信部６とディジタル情報入力部７と固有情報計算部８と第二の電子署名部９とが構成されている。

【００４６】図３は本発明の一実施例による電子透かし挿入処理を示すフローチャートであり、図４は本発明の一実施例によるメディアデータ登録処理を示すフローチャートである。これら図１～図４を参照して本発明の一実施例による電子透かしシステムの動作について説明する。

【００４７】本発明の一実施例による電子透かしシステムはメディアデータに電子透かしを挿入し、そのメディアデータを登録サーバ部３に登録するシステムである。以下、説明の便宜上、静止画データを取上げて行うが、メディアの選択は本質的なものではなく、他のメディアでもそのメディアを扱う適切な機構を準備すれば、本発明の一実施例と同様に処理することが可能である。

【００４８】上記の電子透かしシステムを利用するのに先立って、第一の利用者（メディアデータの供給者）は電子透かしを挿入したい静止画データを準備し、固有情報計算部８と同様の手段を用いてその静止画データの固有情報を求めておく。

【００４９】上記の電子透かしシステムを利用する際、第一の利用者はメディアデータ固有情報入力部１に上記の静止画データの固有情報を入力し、第一の電子署名部２で第一の利用者の電子署名を付与して登録サーバ部３に送る。

【００５０】第一の電子署名部２は、例えば電子メールの作成・送信ソフトウェア等に組込まれていても良く、その場合、第一の電子署名部２から登録サーバ部３にはＳＭＴＰ接続等を用いて署名後のデータが送付されることになる。その他の送信方法による場合にはその方法（あるいはプロトコル）毎に適した電子署名手段の組込み法が存在し得るが、ここでは電子メールをあげるだけにとどめておく。

【００５１】一方、第一の利用者は同時にその静止画データをメディアデータ入力部４に入力する。これは第二の利用者（メディアデータの登録者）がその静止画データを用いるための入力であり、第一の利用者はフロッピディスクや他のリムーバブルメディアを用いて該メディアデータ入力部４に入力することとなる（図３ステップＳ１）。あるいは、上記の電子署名を施した第一の固有情報の転送時と同様に、電子メール等の方法でオンラインで送信することも可能である。入力された静止画データは電子透かし挿入部５及び固有情報計算部８に送られる。

【００５２】固有情報計算部８は入力された静止画データの固有情報を計算し、その固有情報を第二の電子署名部９に渡す（図３ステップＳ２）。第二の利用者はメディアデータ入力部４から入力された静止画データに対して添付したい情報を、ディジタル情報入力部７に入力する。この添付情報は、例えばテキストデータであり、内容としては任意のものが考えられるため、ここでは特に特定しない。

【００５３】ディジタル情報入力部７は第二の利用者が入力した添付情報を第二の電子署名部９に送る。第二の電子署名部９は固有情報計算部８から送られてきた固有情報とディジタル情報入力部７から送られてきた添付情報とを合成し（図３ステップＳ３）、その合成した情報に第二の利用者の電子署名を施して電子透かし挿入部５に出力する（図３ステップＳ４）。

【００５４】電子透かし挿入部５はメディアデータ入力部４から入力される静止画データと、第二の電子署名部９で電子署名が施された添付情報とを受取ると、静止画データに電子署名が施された添付情報を電子透かしとして埋込む（図３ステップＳ５）。添付情報及び固有情報が電子透かしとして埋込まれた静止画データは送信部６に送られ、送信部６から登録サーバ部１３へと送信される。

【００５５】電子透かしを挿入した画像は本システムの第一の利用者が電子透かしをいれようとした用途に沿って用いられる。具体的には、著作権表示であるとか、画像表示のコントロール等であろうが、それらは本発明の目的とするものではないので、その詳細説明は省略する。尚、上記の電子透かしの挿入処理は登録サーバ部３に登録する静止画データ全てに対して行われる（図３ステップＳ１～Ｓ６）。

【００５６】登録サーバ部３は第一の電子署名部２から署名付きの固有情報データが送られてくると（図４ステップＳ１１，Ｓ１２，Ｓ１３）、第一の電子署名部２で施された電子署名と固有情報データとを保持しておく（図４ステップＳ１４）。

【００５７】一方、登録サーバ部３は送信部６から電子透かし入りの静止画データが送られてくると、つまりメディアデータ登録要求であれば（図４ステップＳ１５）、その静止画データに電子署名が施され（図４ステップＳ１６）、このメディアデータ登録要求に対応する固有情報があれば（図４ステップＳ１７）、送信部６から送られてきた静止画データから抽出した固有情報データを保持している固有情報データと比較する（図４ステップＳ１８）。

【００５８】登録サーバ部３では固有情報データの一致を確認した後（図４ステップＳ１９）、送信部６から送られてきた静止画データをデータベースに登録する（図４ステップＳ２０）。具体的には、データベースソフト等への登録を行うことになる。尚、登録サーバ部３では固有情報データの不一致を確認すると（図４ステップＳ１９）、固有情報不一致を第三の単体コンピュータ１３に通知する（図４ステップＳ２２）。

【００５９】また、電子署名の検証に際してはＣＡ（Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ：認証機関）等の外部の存在が必要になるが、その意図・用法等は当業者にとってあきらかであるから、本実施例ではその説明を省略する。尚、上記のメディアデータ登録処理は登録サーバ部３に登録する静止画データ全てに対して行われる（図４ステップＳ１１～Ｓ２２）。

【００６０】図５は本発明の他の実施例によるメディアデータから電子透かしを検出するシステムの構成を示すブロック図である。図において、メディアデータから電子透かしを検出するシステムはメディアデータ入力部２１と、電子透かし抽出部２２と、メディアデータ作成部２３と、固有情報計算部２４と、署名デコード部２５と、ハッシュ計算部２６と、データベース部２７と、ハッシュ値比較部２８と、出力選択部２９とから構成されている。

【００６１】メディアデータ入力部２１は電子透かしを検出する対象となるメディアデータの入力手段である。これは、例えば静止画ならば、ＪＰＥＧやＴＩＦＦといったフォーマットのデータを入力する手段にあたる。より具体的には、例えばコンピュータ上のディスク装置やネットワーク等のデータ入力手段、あるいはスキャナ装置等を用いた画像取込み手段に相当する。

【００６２】電子透かし抽出部２２はメディアデータ入力部２１に与えられたメディアデータから、電子透かしとして埋められている情報を抽出する。電子透かしには本発明の一実施例で述べたように、様々な方法が存在し、それら個々について専用の抽出手段が必要である。その抽出方法については本発明の目的とするものではなく、個々の技術によるものであるから、ここでは詳細な説明を行わない。

【００６３】メディアデータ作成部２３はメディアデータ入力部２１で入力されたメディアデータから、電子透かし抽出部２２で抽出された電子透かしを除去したメディアデータを作成する。より具体的には、電子透かし抽出部２２と同一のプログラムモジュールで実行されて両方の出力を得る等のインプリメンテーションも考えられる。

【００６４】固有情報計算部２４はメディアデータ作成部２３で作成されたメディアデータから、メディアデータの固有情報を計算する。固有情報の実例としては、例えば上記の文献５に記載されているように、静止画データをブロック単位に細分化し、各ブロックでＤＣＴ係数を求めてその低周波成分を固有情報とする等の方法がある。

【００６５】データベース部２７はメディアデータの固有情報から、少なくともその固有情報が関連付けられているデータが検索可能に構成されており、電子署名を検査するために必要な情報（例えば、上記のメディアデータに付されたディジタル情報）をも検索可能となっている。当然、少なくとも検索に先立って関連する情報が格納されている必要がある。電子署名の検証に必要な情報としては、例えば署名者に関する情報を与えておけばよく、検証用のキーについてはデータベース部２７に格納しないで、鍵配送センタ（図示せず）等の機構を導入して入手することも可能である。本発明では検証鍵情報までもこのデータベース部２７に格納されているものとする。

【００６６】署名デコード部２５は固有情報と電子透かしとが入力されると、与えられた固有情報を基にデータベース部２７から検証用情報を検索する。検証用情報には種々のものが考えられるが、ここでは少なくとも電子署名をデコードするに足る情報が与えられるものとし、署名デコード部２５はその情報、すなわちデコードのための鍵を受取り、受取った鍵によって電子透かしをデコードし、メディアデータの固有情報と電子署名を検査するために必要な情報とのハッシュ値をデコード結果として出力する。

【００６７】ハッシュ計算部２６は固有情報計算部２４から得たメディアデータの固有情報から、データベース部２７を検索して得られた情報と検索に用いた固有情報とを用いてハッシュ値を計算する。ここでは本システムで用いる電子署名の方式がハッシュを使うことを想定しているため、ハッシュ値を計算するとしている。

【００６８】ハッシュ値比較部２８は二つの数値入力を比較し、その関係を出力する。ここでいう比較とは、例えばもっとも単純な形では一致するか否かの判定情報である。出力選択部２９はハッシュ値比較部２８の出力に基づいて何らかの情報の出力や不出力を選択する。ここでは、当該情報源を表記していないが、例えばこの出力選択部２９をネットワークを介して情報の閲覧端末に接続しておき、閲覧端末での情報表示の制御に用いることもできる。

【００６９】図６は本発明の他の実施例によるメディアデータから電子透かしを検出する処理動作を示すフローチャートである。これら図５及び図６を参照して本発明の他の実施例によるメディアデータから電子透かしを検出する処理動作について説明する。

【００７０】まず、利用者による当該システムの利用に先立って、データベース部２７にはメディアデータの固有情報を検索キーとして用いる際に、少なくとも検証用の鍵情報とさらに別のディジタル情報とが検索可能なように、予め各種データが貯えられているものとする。この各種データの蓄積は利用者ではなく、システム管理者が行う。

【００７１】利用者が、まず、メディアデータ入力部２１に電子透かしが入っていると思われるメディアデータを入力すると（図６ステップＳ３１）、その入力されたメディアデータからは電子透かし抽出部２２によって電子透かしが抽出される（図６ステップＳ３２）。電子透かし抽出部２２で抽出された電子透かしは署名デコード部２５に送られるとともに、それらメディアデータ及び抽出された電子透かしはメディアデータ作成部２３へ送られる。ここからの処理の流れは二分岐しているので、片方ずつ説明する。

【００７２】メディアデータ作成手段２３はメディアデータ作成部２３へ送られたメディアデータ及び電子透かしから、電子透かしを取除いたメディアデータを作成する（図６ステップＳ３３）。電子透かしが取除かれたメディアデータは固有情報計算部２４へと送られ、固有情報計算部２４でそのメディアデータに対する固有情報が求められる（図６ステップＳ３４）。求められた固有情報はハッシュ計算部２６へと送られる。

【００７３】ハッシュ計算部２６は固有情報計算部２４から受取った固有情報を検索キーとしてデータベース部２７からその固有情報に対応して登録されている情報を得てから、それら固有情報及びその情報を合わせたデータからハッシュ値を計算する（図６ステップＳ３６）。

【００７４】一方、署名デコード部２５はもう一方の処理の流れから得られた固有情報を検索キーとしてデータベース部２７を検索し、署名の検証用鍵を入手する。それによって、電子透かし抽出部２２から受取った電子透かしをデコードする（図６ステップＳ３５）。

【００７５】ハッシュ値比較部２８は署名デコード部２５のデコード結果とハッシュ計算部２６で計算されたハッシュ値とを比較し（図６ステップＳ３７）、出力選択部２９はハッシュ値比較部２８での比較結果に基づいて出力を制御するための動作を行う。

【００７６】すなわち、出力選択部２９はハッシュ値比較部２８での比較結果が一致ならば（図６ステップＳ３８）、それらが一致した時の処理（例えば、出力許可の送出処理等）を実行する（図６ステップＳ３９）。また、出力選択部２９はハッシュ値比較部２８での比較結果が不一致ならば（図６ステップＳ３８）、それらが不一致した時の処理（例えば、出力不許可の送出処理等）を実行する（図６ステップＳ４１）。尚、上記の電子透かし検出処理はメディアデータ入力部２１に入力されたメディアデータ全てに対して行われる（図６ステップＳ３１～Ｓ４１）。

【００７７】本発明の他の実施例は、特に本発明の一実施例による登録方式・システムと合わせて用いることを前提としている。そのため、データベース部２７で合わせて登録されているディジタル情報を、本発明の一実施例のディジタル情報入力部７で与えられるものと同一とすることで、メディアデータの固有値とそれに合わせられたディジタル情報との同一性を検証することができる。

【００７８】本発明の一実施例及び他の実施例は、例えばネットワーク上でコンテンツを公開して一般ユーザが閲覧する場合、何らかの閲覧制限情報を付与したい時等に用いることができる。その場合のディジタル情報とは、閲覧の制限のための情報であり、出力選択部２９の出力はブラウザへの表示・非表示の制御のためのデータということになる。

【００７９】ここで、図示していないが、上述した本発明の一実施例及び他の実施例に示すシステムを二つ以上用い、それらのシステムで得られる結果の多数決をとることで、特定のサーバの不正を防止することもできる。

【００８０】また、本発明の一実施例及び他の実施例では電子署名を施す際にハッシュを取ることを前提としているが、電子署名を施す際に任意の一方向性関数をとり、ハッシュ計算部２６の代わりに任意の一方向性関数による計算手段を用いても実現することができる。

【００８１】このように、電子透かしとメディアデータ自身との関係を電子透かしの一部として取入れ、さらに電子署名を施すことによって、電子透かしとメディアデータとを分離したり、容易に内容を改竄することができなくすることが可能となる。

【００８２】また、元のメディアデータの配布が当該メディアデータの登録サーバ部３への登録時のみとなるので、元のメディアデータの配布範囲を必要最小限とすることができ、元のメディアデータの流出をより強く防止することができる。

【００８３】さらに、上述した本発明の一実施例及び他の実施例に示すシステムを二つ以上用い、それらのシステムで得られる結果の多数決をとることで、特定のサーバの不正を防止しやすくすることができる。

【００８４】

【発明の効果】以上説明したように本発明によれば、メディアデータに電子透かしを挿入する電子透かしシステムにおいて、外部から入力されかつメディアデータを特定する固有情報に第一の電子署名を施し、外部から入力されたメディアデータからメディアデータを特定する固

有情報を計算し、その固有情報とメディアデータに添付すべき添付情報との合成情報に第二の電子署名を施して電子透かしとしてメディアデータに埋込み、第一の電子署名が施こされた固有情報と第二の電子署名が施こされた固有情報とを比較しかつその比較結果に応じてメディアデータをデータベースに登録することによって、元のメディアデータをあまり流出させることなく、元のメディアデータと埋め込まれた電子透かしとを分離しにくくすることができ、電子透かしの挿入・検出等を複数のサーバやクライアントに分散した場合でも改竄者を特定することができるという効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例による電子透かしシステムの構成を示すブロック図である。

【図２】本発明の一実施例による電子透かしシステムのシステム構成を示すブロック図である。

【図３】本発明の一実施例による電子透かし挿入処理を示すフローチャートである。

【図４】本発明の一実施例によるメディアデータ登録処理を示すフローチャートである。

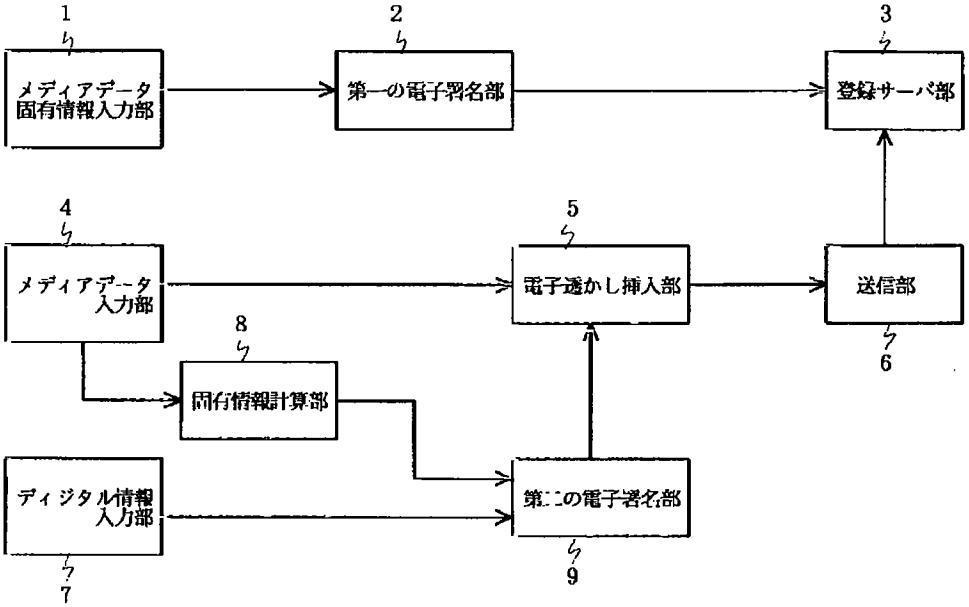
【図５】本発明の他の実施例によるメディアデータから電子透かしを検出するシステムの構成を示すブロック図である。

【図６】本発明の他の実施例によるメディアデータから電子透かしを検出する処理動作を示すフローチャートである。

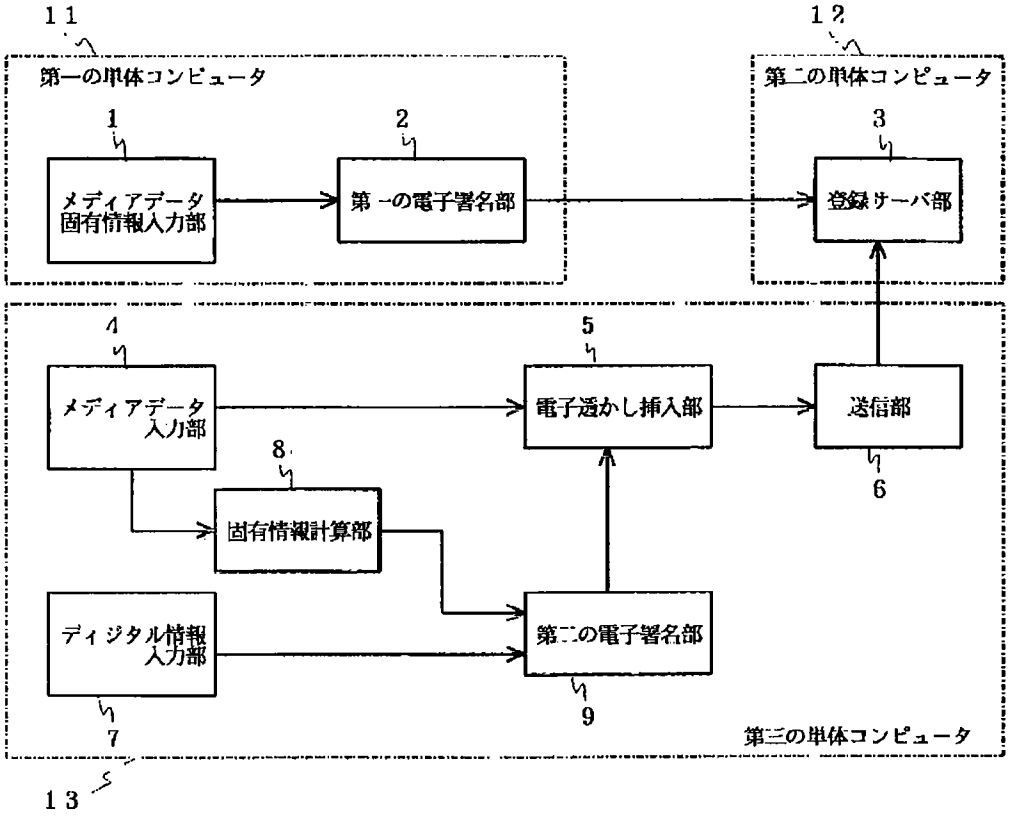
【符号の説明】

１　メディアデータ固有情報入力部
２　第一の電子署名部
３　登録サーバ部
４　メディアデータ入力部
５　電子透かし挿入部
６　送信部
７　ディジタル情報入力部
８　固有情報計算部
９　第二の電子署名部
１１　第一の単体コンピュータ
１２　第二の単体コンピュータ
１３　第三の単体コンピュータ
２１　メディアデータ入力部
２２　電子透かし抽出部
２３　メディアデータ作成部
２４　固有情報計算部
２５　署名デコード部
２６　ハッシュ計算部
２７　データベース部
２８　ハッシュ値比較部
２９　出力選択部

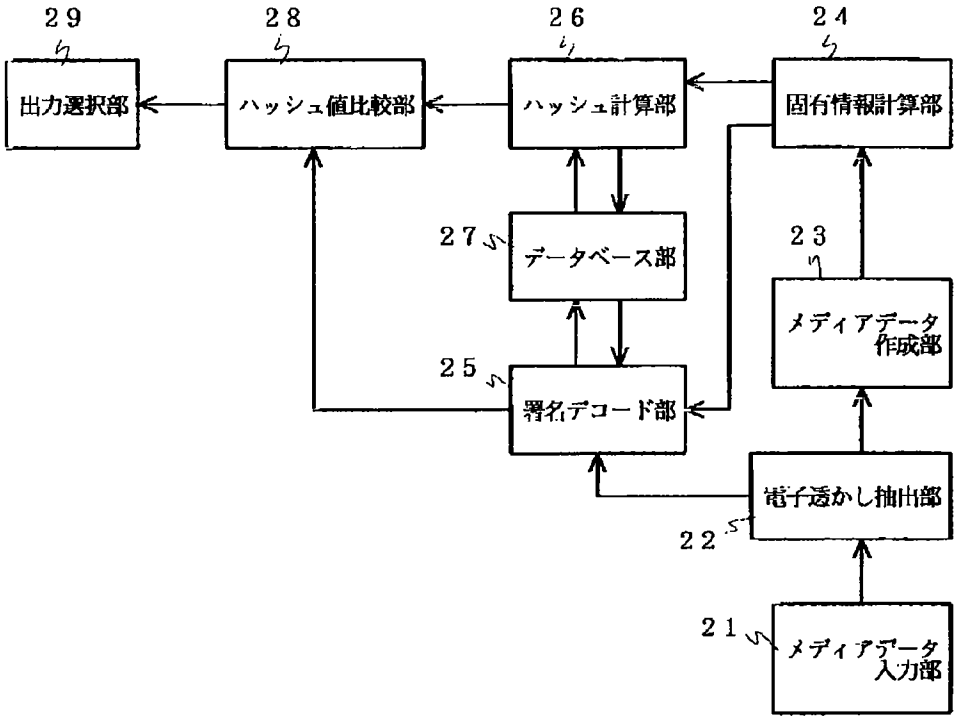
【図１】



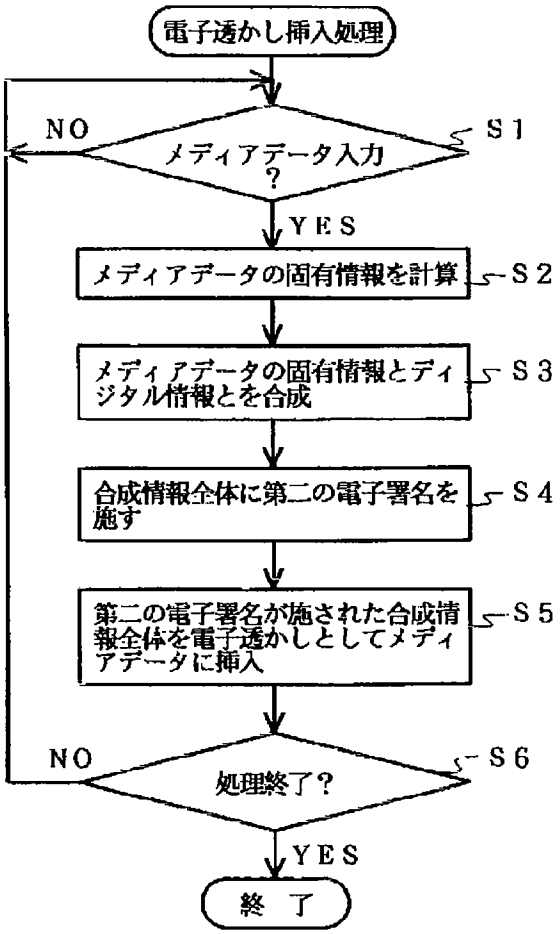
【図２】


１１
第一の単体コンピュータ
１
メディアデータ固有情報入力部
２
第一の電子署名部
１２
第二の単体コンピュータ
３
登録サーバ部
４
メディアデータ入力部
５
電子透かし挿入部
送信部
６
８
固有情報計算部
ディジタル情報入力部
７
第二の電子署名部
９
第三の単体コンピュータ
１３

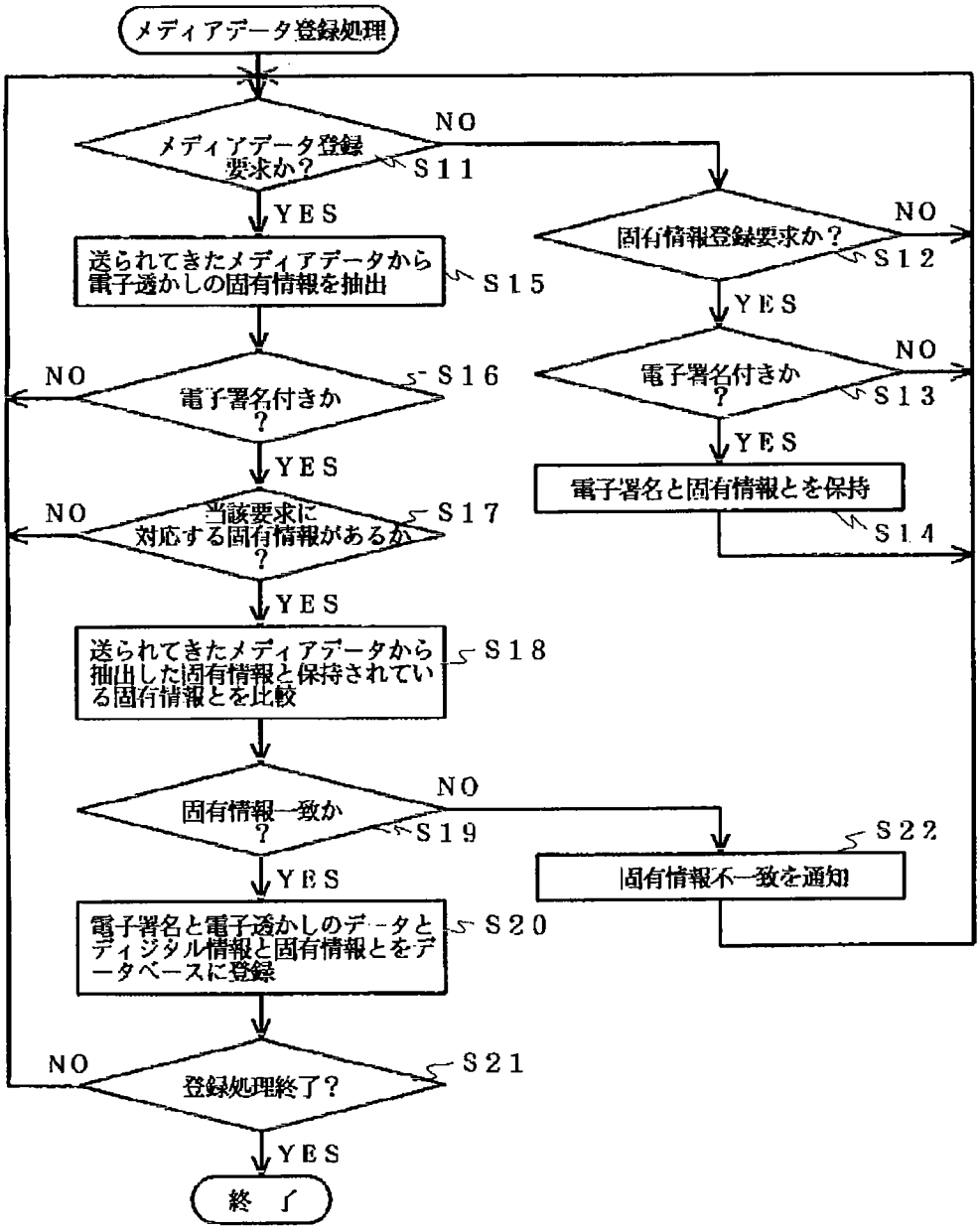
【図５】


２９
出力選択部
２８
ハッシュ値比較部
２６
ハッシュ計算部
２４
固有情報計算部
２７
データベース部
２３
メディアデータ作成部
２５
署名デコード部
電子透かし抽出部
２２
２１
メディアデータ入力部

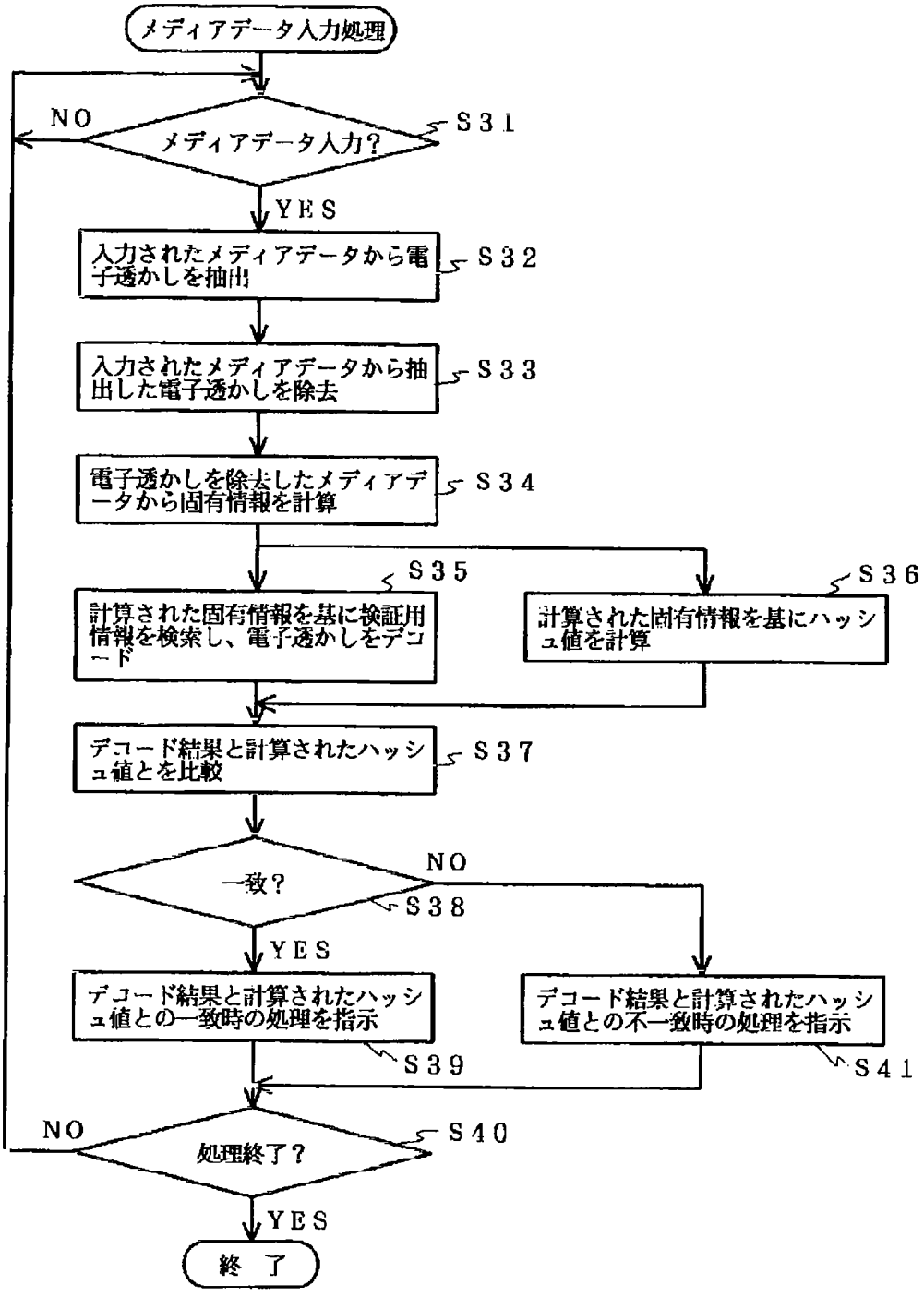
【図3】


電子透かし挿入処理
NO
メディアデータ入力？
S1
YES
メディアデータの固有情報を計算
S2
メディアデータの固有情報とディジタル情報とを合成
S3
合成情報全体に第二の電子署名を施す
S4
第二の電子署名が施された合成情報全体を電子透かしとしてメディアデータに挿入
S5
NO
処理終了？
S6
YES
終　了

【図4】


メディアデータ登録処理
メディアデータ登録要求か？
S11
NO
YES
固有情報登録要求か？
S12
NO
YES
送られてきたメディアデータから電子透かしの固有情報を抽出
S15
電子署名付きか？
S13
NO
YES
電子署名と固有情報とを保持
S14
電子署名付きか？
S16
NO
YES
当該要求に対応する固有情報があるか？
S17
NO
YES
送られてきたメディアデータから抽出した固有情報と保持されている固有情報とを比較
S18
固有情報一致か？
S19
NO
YES
固有情報不一致を通知
S22
電子署名と電子透かしのデータとディジタル情報と固有情報とをデータベースに登録
S20
登録処理終了？
S21
NO
YES
終了

【図6】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
H04N	7/08		G06F	15/66	B
	7/081		H04N	7/08	Z
	7/173				